UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,909	04/06/2006	Vincent Carlier	4005-0277PUS1	7126

2292 7590 01/09/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	
NOTIFICATION DATE	**DELIVERY MODE**
01/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	**Application No.** 10/574,909	**Applicant(s)** CARLIER ET AL.	
	Examiner Christian La Forgia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 April 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The amendment of 15 October 2007 has been noted and made of record.

2. Claims 1-5 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-5 have been considered but are moot in view of the new grounds of rejection presented in response to the Applicant's amendments.

4. See further rejections set forth below.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. If the broadest reasonable interpretation of the claimed invention as a whole encompasses a human being, the claim must be rejected as directed to nonstatutory subject matter. See MPEP § 2105. The Applicant's addition of "before introduction in a device" could lead one of ordinary skill to interpret the method claim as being performed by a human being. For example, the separating the algorithm into the form of initial polynomials of at least two variables each and having a degree of not less than two could be interpreted as a human operator factoring a cryptographic mathematical equation into separate polynomials. This is further compounded by the combination of the polynomials and implementing the combined polynomials in the programmable processor unit, which are also capable of being performed by a human. Since the broadest reasonable interpretation of the

claimed invention encompasses method steps performed by a human being, the claims are directed toward nonstatutory subject matter.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0187035 to Schwan et al., hereinafter Schwan, in view of U.S. Patent Application Publication No. 2004/0071293 A1 to Yamamichi et al., hereinafter Yamamichi, and further in view of U.S. Patent No. 7,233,662 B2 to Futa et al., hereinafter Futa.

9. As per claim 1, Schwan teaches a method of protecting a cryptographic algorithm (paragraphs 0007, 0013, i.e. destroying or erasing a cryptographic algorithm so an unauthorized person does not obtain knowledge of the algorithm) for execution in a device comprising programmable processor unit (paragraph 0010, microprocessor and programmable memory), wherein the algorithm can either symmetric or asymmetric (paragraph 0015) and implemented on the programmable processing unit (paragraph 0002).

10. Schwann teaches that any type of cryptographic method may be used, including symmetric and asymmetric cryptographic methods.

11. Schwann does not teach protecting the cryptographic algorithm before introduction in a device by separating the algorithm into initial polynomials and combining those polynomials in the device to be executed by the processor unit.

12. Yamamichi discloses an encryption algorithm that is based on a polynomial calculation using the random number polynomial and the public key polynomial that is based on the NTRU algorithm (paragraph 0075).

13. It would have been obvious to one of ordinary skill in the art at the time the invention was made to replace the cryptographic methods disclosed in Schwann with the NTRU algorithm as disclosed in both Yamamichi and Futa, thereby protecting the cryptographic algorithm since NTRU splits it into polynomials, since Futa states at column 1, lines 35-42 that the NTRU algorithm can be installed on low-performance CPUs such as those found in household appliances, thereby ensuring additional security for devices similar to those disclosed in Schwan.

14. Regarding claim 2, Schwan teaches the step of storing the encryption algorithms in the form of a configuration file that is loaded into a memory associated with the processor unit (paragraph 0002, i.e. updating the control program, programming the control unit to a customer and application needs, modify the functional and performance range of the control unit, reprogramming the control unit).

15. With regards to claim 3, Schwan teaches wherein the memory and the programmable processor unit are associated with an eraser member serving, in the event of an intrusion into the device, to erase the processor unit, and to erase the memory containing the configuration file when the configuration is present in said memory (paragraph 0013, i.e. encryption algorithm is erased and/or destroyed after the housing is opened (the intrusion)).

16. Regarding claim 4, Schwan discloses the use of DES (paragraph 0013). As noted above DES combines more than two initial polynomials in order to obtain combined polynomials. DES also includes a function f_k and f_k^{-1}. This is supported by the disclosure of DES in **Cryptography and Network Security, Principles and Practices**, by William Stallings, hereinafter Stallings. Specifically, Stallings discloses the function f_k on at least page 61, or the initial permutation as disclosed on page 57. Stallings goes on further to discuss on page 57 the inverse initial permutation towards the end of the cryptographic calculation. Therefore Schwan teaches the step of combining each combined polynomial (Q_k) with a function (f_k), and of combining the following combined polynomial (Q_{k+l}) with an inverse function (f_k^{-1}) in his disclosure of DES.

17. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schwan in view of Yamaichi in view of Futa as applied above and in further view of **Applied Cryptography, Protocols, Algorithms, and Source Code in C**, by Bruce Schneier, hereinafter Schneier.

18. With regards to claim 5, Schwan does not teach wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the initial permutation, or claimed function f_k, be a linear function, since Schneier states at page 271 that the initial permutation is used to transpose the input block of data, and as such a linear function would make it easier to transpose the input block and load the plaintext and ciphertext into a DES chip in byte-sized pieces.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

21. The following patents are cited to further show the state of the art with respect to NTRU cryptographic method, such as:

United States Patent No. 7,110,548 B1 to Ougi et al., which is cited to show distributing an encryption algorithm.

United States Patent Application Publication No. 2004/0260950 A1 to Ougi et al., which is cited to show distributing an encryption algorithm (paragraphs 0008, 0011).

United States Patent No. 6,058,478 A to Davis, which is cited to show updating a cryptographic algorithm (see claim 8).

United States Patent Application Publication No. 2003/0081770 A1 to Futa et al., which is cited to show the published application that supplied the motivation for the above combination.

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

23. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

Clf